



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/805,729	03/22/2004	Phillip Andrew Porras	SRI/3928-9	9573

52197 7590 12/18/2007
PATTERSON & SHERIDAN, LLP
SRI INTERNATIONAL
595 SHREWSBURY AVENUE
SUITE 100
SHREWSBURY, NJ 07702

EXAMINER

HOFFMAN, BRANDON S

ART UNIT	PAPER NUMBER
----------	--------------

2136

MAIL DATE	DELIVERY MODE
-----------	---------------

12/18/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

AK

Office Action Summary	Application No. 10/805,729	Applicant(s) PORRAS ET AL.	
	Examiner Brandon S. Hoffman	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 12 October 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>10-25-04 & 04-27-06</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-20 are pending in this office action.
2. Applicant's arguments, filed October 12, 2007, have been fully considered but they are not persuasive.

Information Disclosure Statement

3. The information disclosure statements (IDS's) submitted on October 25, 2004, and April 27, 2006, are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 102

5. Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Vaidya (U.S. Patent No. 6,279,113).

Regarding claims 1, 19, and 20, Vaidya teaches a method/computer-readable medium/apparatus for performing network surveillance, said method comprising the steps of:

- Receiving a plurality of network packets handled by a network entity (col. 5, lines 26-46);
- Building at least one statistical profile from at least one measure of said plurality of network packets (col. 6, lines 1-11); and
- Analyzing said at least one statistical profile to detect suspicious network activity (col. 6, lines 11-26).

Regarding claim 2, Vaidya teaches wherein said at least one measure monitors data transfers by monitoring network packet data transfer commands (col. 5, lines 33-39, data transport).

Regarding claim 3, Vaidya teaches wherein said at least one measure monitors data transfers by monitoring network packet data transfer errors (col. 5, lines 33-39, unauthorized attempts to access network objects).

Regarding claim 4, Vaidya teaches wherein said at least one measure monitors data transfers by monitoring network packet data transfer volume (col. 5, lines 33-39).

Regarding claim 5, Vaidya teaches wherein said at least one measure monitors network connections by monitoring network connection requests (col. 7, lines 33-36).

Regarding claim 6, Vaidya teaches wherein said at least one measure monitors network connections by monitoring network connection denials (col. 5, lines 33-39, attempted delivery of malicious data packets).

Regarding claim 7, Vaidya teaches wherein said at least one measure monitors network connections by monitoring a correlation of network connection requests and network connection denials (col. 5, lines 33-39 and col. 7, lines 33-36).

Regarding claim 8, Vaidya teaches wherein said at least one measure monitors errors by monitoring at least one error code included in a network packet, wherein said at least one error code comprises a privilege error code or an error code indicating a reason a packet was rejected (col. 5, lines 33-39, unauthorized attempts to access network objects).

Regarding claim 9, Vaidya teaches further comprising the step of responding based on determining whether said at least one statistical profile indicates suspicious network activity (fig. 3, ref. num 66).

Regarding claim 10, Vaidya teaches wherein said responding step comprises transmitting an event record to a network monitor (col. 7, lines 52-67).

Regarding claim 11, Vaidya teaches wherein said transmitting the event record to a network monitor step comprises transmitting the event record to a hierarchically higher network monitor (col. 5, lines 47-51).

Regarding claim 12, Vaidya teaches wherein said transmitting the event record to a network monitor step comprises transmitting the event record to a network monitor that receives event records from a plurality of network monitors (fig. 1, ref. num 12).

Regarding claim 13, Vaidya teaches wherein said network monitor that receives event records from said plurality of network monitors comprises a network monitor that correlates activity in said plurality of network monitors based on said received event records (col. 5, lines 26-46).

Regarding claim 14, Vaidya teaches wherein said responding step comprises altering said analysis of said plurality of network packets (col. 7, lines 31-45).

Regarding claim 15, Vaidya teaches wherein said responding step comprises severing a communication channel (col. 6, lines 21-26).

Regarding claim 16, Vaidya teaches wherein said network entity comprises at least one of a gateway, a router, a proxy server, a firewall, and a virtual private network (VPN) entity (fig. 1, ref. num 20).

Regarding claim 17, Vaidya teaches wherein said plurality of network packets are partitioned into a plurality of sessions representing a communication transaction between two hosts (col. 7, line 52 through col. 8, line 15).

Regarding claim 18, Vaidya teaches wherein said at least one measure monitors network connections by monitoring a source port number and a destination port number included in one of said network packets (col. 2, lines 15-30).

Response to Arguments

6. Applicant argues that Vaidya does not teach building a statistical profile and analyzing the statistical profile to detect suspicious network activity (page 7).

Regarding applicant's arguments, examiner disagrees. While it is true that Vaidya never mentions "statistical" or any other variation, according to applicant, Vaidya does teach the idea of building a profile from monitored data, and using that profile to detect suspicious network activity. Column 9, lines 3-20, shows

If the server is being monitored, in step 100 a session list in the state cache 44 is searched for a matching entry. Application information and the server IP address extracted from the packet into the register cache 40 are used to calculate a hash index, and the hash index is used to search for a matching entry from the session list. In step 102, it is determined whether a matching session entry

was found. If a matching session entry is found, the entry is returned to the virtual processor 36 in step 104. The session entry might contain a record of timer/counter expressions executed on packets associated with the application session. For instance, the entry might reflect that within the application session a particular file within the application has been accessed ten times in the past twenty minutes. The virtual processor 36 uses this timer/counter information to determine whether a network intrusion is associated with the particular packet. The state cache 44 is also utilized to create a record of executed expressions in a sequential attack signature profile.

This shows that a record is created based on monitored activities (in this case, the number of accesses of a file within a given time period) and the monitored activities indicate if a network intrusion is taking place.

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Brandon Hoffman/

BH

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


12,17,07